

REMARKS

This response is submitted in reply to the Office Action dated March 7, 2006. Claims 1, 13, 14 and 21-23 were rejected under 35 U.S.C. 112, second paragraph, and claims 1 – 23 were rejected under 35 U.S.C. 103(a). In response, Applicants have amended claims 1, 5, 13-14 and 21-23 to clarify the claim language. No new matter has been introduced as a result of the amendments. Applicants respectfully traverses the rejections. Favorable reconsideration is requested. A Request for Continued Examination is submitted herewith. The Commissioner is hereby authorized to charge deposit account 02-1818 for any fees which are due and owing.

Applicants thank Examiner Colin for granting a telephonic interview to Applicants' representative, MacLane C. Key, on June 1, 2006. The rejections under 35 U.S.C. 112 and 35 U.S.C. 103(a) were discussed with respect to Claim 1. Agreement was not reached.

Claims 1, 13-14 and 21-23 were rejected under 35 U.S.C. 112, second paragraph, as failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, the Office Action stated that Claims 1, 13, 14, 21 and 23 lacked antecedent basis for "the authentication between the medium and a server". Applicants respectfully submit that the above quoted limitation was only present in Claim 1 and that Claim 1, as amended, no longer recites this language. Accordingly, Applicants respectfully submit that this rejection is overcome and therefore respectfully request that such rejection be withdrawn.

Further, the Office Action indicated that the information processing apparatus authenticating the user using the private key corresponding to the user in Claims 1, 13-14, 21 and 23 was unclear. Applicants have amended these claims to make their meaning more clear. Accordingly, Applicants respectfully submit that this rejection is overcome and therefore respectfully request that such rejection be withdrawn.

Claims 1-23 were rejected as being unpatentable over U.S. Patent No. 6,694,436 to Audebert ("Audebert"). Applicants respectfully traverse this rejection, as the cited reference fails to disclose or suggest the features claimed in the present invention. Favorable reconsideration is respectfully requested.

Claim 1 is directed to a user authentication system, including a data holding medium for holding a common key corresponding to a user, used in a common-key encryption method for authentication between the data holding medium held by the user and an authentication

apparatus. The authentication apparatus is configured for holding the common key used in the common-key encryption method and a private key corresponding to the user used in a public-key encryption method for authentication between the data holding medium and a server to perform a service to the user. The system also includes an information processing apparatus connected to the authentication apparatus in an always-communicable manner and provided with a function for performing authentication by the public-key encryption method. The authentication apparatus is configured to receive a first data item. The first data item is associated with a first authentication request from said information processing apparatus. The authentication apparatus is configured to authenticate the data holding medium by using the common key in response to the first authentication request. The authentication apparatus is further configured to encrypt, only if the data holding medium is authenticated in response to the first authentication request, the first data item using the private key associated with the user and to send the encrypted first data item to the information processing apparatus. The information processing apparatus is configured to decrypt the encrypted first data item using a public key associated with the user and to compare the decrypted result with the first data item. The authentication apparatus performs authentication, authenticating the data holding medium by using the common key used in the common-key encryption method for the user held by the data holding medium, in response to an additional authentication request sent from the information processing apparatus. The additional authentication request is sent only if the decrypted result corresponds to the first data item. Only when the user has been authenticated in response to the additional authentication request, the authentication apparatus performs processing, using the private key corresponding to the user, for making the information processing apparatus authenticate the user. Information encrypted by the public-key encryption method, which is sent from the information processing apparatus and forwarded to the authentication apparatus, is decrypted by the authentication apparatus using the private key corresponding to the user so as to obtain decrypted information. The decrypted information is encrypted by the authentication apparatus using the common key. The obtained common key encrypted information is sent back to the data holding medium.

Audebert discloses a terminal which includes a terminal module and a personal security device. The terminal module is adapted to receive high-level requests from an application installed on an electronic unit. The high-level requests are independent of the personal security

device. The terminal module and/or the personal security device includes a reprogrammable memory for storing and a unit for executing a filter program which translates the high-level requests. The filter program includes a unit for identifying and/or authenticating the source of requests sent by the application installed in the electronic unit transaction that is signed by the terminal module using a private key held by a card. Audebert also discloses an exchange where the terminal module decrypts the private key, signs the transaction by means of the private key, destroys the private key and sends the signed transaction to the PC which sends the transaction to the server. Further, Audebert discloses that a secure communication channel can be created between the terminal and the integrated circuit card.


However, it is respectfully submitted that Audebert does not disclose or suggest receiving a first data item, wherein the data item is associated with a first authentication request from the server, encrypting the first data item using a private-key of the user and sending the encrypted data item to the server, wherein the server decrypts the data item using a public-key of the user and compares the decryption result with the data item. Audebert describes signing a transaction with a private key, but not encrypting a data item associated with an authentication request from the server and sending the encrypted data item to the server to be decrypted with a public key and compared with a copy of the data item at the server.

For at least these reasons, Applicants respectfully submit that Claim 1, and Claims 2-4, which depend from Claim 1, are each patentably distinct over Audebert and in condition for allowance. For similar reasons, Applicants respectfully submit that Claims 5, 13, 14 and 21-23 and Claims 6-12, which depend from Claim 5, and Claims 15-20, which depend from Claim 14, are each patentably distinct over Audebert and in condition for allowance.

In light of the above, Applicants respectfully submit that Claims 1-23 are patentable over the art of record. Accordingly, Applicants respectfully request that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

BY



Thomas C. Basso (46,541)
Customer No. 29175

Dated: June 6, 2006